The University of Texas at Tyler

Information Technology
Access Management Audit

August 2018

THE UNIVERSITY OF TEXAS AT TYLER
OFFICE OF AUDIT AND CONSULTING SERVICES
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

BACKGROUND

Access management is a key control for information technology (IT) and should be carefully managed, including the timely removal of access for former employees. The University of Texas at Tyler (UT Tyler) university-wide risk assessment identified access management for part-time employees as a critical risk; therefore, an audit of the process of monitoring and removing access was included in the Fiscal Year 2018 Annual Audit Plan and approved by the Institutional Audit Committee.

Departments are required to submit termination forms in PeopleSoft, the UT Tyler Human Resource and Financial Management System, when an individual's employment ends. This procedure ends the employee's automatic payroll process and is also used to notify the Information Security Office (InfoSec) who then removes employee's IT access. Part-time employees are paid only if timecards are processed for the employee. Therefore, their termination records may not be initiated timely in PeopleSoft, allowing their IT access account to remain active after their last paycheck.

Beginning July 2017, InfoSec implemented a process to monitor deactivation of IT access for part-time employees who are no longer working at UT Tyler. The process includes sending an email to administrative assistants at the end of the Fall and Spring semesters containing a list of part-time employees who are active in PeopleSoft. The administrative assistants are asked to confirm that the individuals are still working in the department. If an individual is identified as no longer employed by the department, InfoSec deactivates their access and reminds the administrative assistant to submit the required termination form in PeopleSoft. InfoSec is expanding the monitoring to also include summer semesters.

AUDIT OBJECTIVE

The objective of the audit was to determine if UT Tyler's InfoSec monitoring of part-time employees' access was thorough, effective, and a valuable use of InfoSec resources.

STANDARDS

The audit was conducted in accordance with guidelines set forth in *The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing* and *Generally Accepted Government Auditing Standards*.

SCOPE AND METHODOLOGY

To accomplish the objectives noted above, the following procedures were conducted for Spring 2017, Fall 2017 and Spring 2018:

- Gained an understanding of UT Tyler procedures for terminating part-time employees in PeopleSoft and deactivating their IT access.

- Tested InfoSec's monitoring and access removal for part-time employees by:
    - Obtaining the lists of part-time employees developed for InfoSec by the Human Resources Department,
    - Comparing the list to the InfoSec monitoring spreadsheet to determine if all active part-time employees were included,
    - Obtaining a sample of emails from InfoSec to the administrative assistants to confirm all part-time employees were included for review,
    - Verifying InfoSec followed up with administrative assistants who did not respond, and
    - Testing a sample of administrative assistants' responses and the resulting action taken by InfoSec.
- Verified access had been removed by testing a sample of inactive part-time employees recorded in the PeopleSoft Human Capital System (HCS) provided by the data analytics specialist from the University of Texas System Internal Audit Office to the list of active user accounts.

Our procedures did not include testing access removal for former full-time employees. This is not considered a high risk since the procedures required to terminate their payroll process are also used by InfoSec to remove the employee's IT access.

AUDIT RESULTS

According to The University of Texas System Audit Office, *"A Priority Finding is defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated.*

Finding Level Legend	
Priority	*A finding is defined as an issue that if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Tyler.*
High	*A finding that is considered to have a medium to high probability of adverse effects to UT Tyler as a whole or to a significant college or department.*
Medium	*A finding that is considered to have a low to medium probability of adverse effects to UT Tyler as a whole or to a college or department.*
Low	*A finding that is considered to have a minimal probability of adverse effects to UT Tyler as a whole or to a college or department.*

This audit resulted in **no** findings.

RESULTS

InfoSec monitors access removal for part-time employees using lists obtained from the Human Resource Department and responses from administrative assistants. Testing results show InfoSec is following their procedures which resulted in deactivation of 229 user accounts for terminated part-time employees' for which forms were not submitted timely in PeopleSoft. This represents 36% of the 634 part-time user accounts whose access was removed at the end of the three semesters tested.

CONCLUSION

UT Tyler's Information Security Office's continuous monitoring is thorough, effective and is a valuable use of InfoSec resources. We commend the InfoSec for developing this monitoring process and their efforts to mitigate this critical risk. We appreciate their assistance during this project.